Subpart 1852.2—Texts of Provisions and Clauses

1852.203–70 Display of Inspector General Hotline Posters.

As prescribed in 1803.7001, insert the following clause:

DISPLAY OF INSPECTOR GENERAL HOTLINE POSTERS (JUN 2001)

(a) The Contractor shall display prominently in common work areas within business segments performing work under this contract, Inspector General Hotline Posters available under paragraph (b) of this clause.

(b) Inspector General Hotline Posters may be obtained from NASA Office of Inspector General, Code W, Washington, DC, 20546–0001, (202) 358–1220.

[66 FR 29727, June 1, 2001]

1852.204–74 Central Contractor Registration.

As prescribed in 1804.7404, insert the following clause:

CENTRAL CONTRACTOR REGISTRATION (MAY 2002)

(a) *Definitions.* As used in this clause—

(1) ''Central Contractor Registration (CCR) database'' means the primary DoD repository for contractor information required for the conduct of business with NASA.

(2) ''Data Universal Number System (DUNS) number'' means the 9-digit number assigned by Dun and Bradstreet Information Services to identify unique business entities.

(3) ''Data Universal Numbering System +4 (DUNS+4) number'' means the DUNS number assigned by Dun and Bradstreet plus a 4-digit suffix that may be assigned by a parent (controlling) business concern. This 4-digit suffix may be assigned at the discretion of the parent business concern for such purposes as identifying sub-units or affiliates of the parent business concern.

(4) ''Commercial and Government Entity Code (CAGE Code)'' means—

(i) A code assigned by the Defense Logistics Information Service (DLIS) to identify a commercial or Government entity; or

(ii) A code assigned by a member of the North Atlantic Treaty Organization (NATO) that is recorded and maintained by DLIS in the CAGE master file.

(5) ''Registered in the CCR database'' means that all mandatory information, including the DUNS number or the DUNS+4 number, if applicable, and the corresponding CAGE code, is in the CCR database; the DUNS number and the CAGE code have been validated; and all edits have been successfully completed.

(b)(1) By submission of an offer, the offeror acknowledges the requirement that a prospective awardee must be registered in the CCR database prior to award, during performance, and through final payment of any contract resulting from this solicitation, except for awards to foreign vendors performing work outside of the United States.

(2) The Contracting Officer will verify that the offeror is registered in the CCR database.

(3) Lack of registration in the CCR database will make an offeror ineligible for award after March 31, 2001.

(4) DoD has established a goal of registering an applicant in the CCR database within 48 hours after receipt of a complete and accurate application via the Internet. However, registration of an applicant submitting an application through a method other than the Internet may take up to 30 days. Therefore, offerors that are not registered should consider applying for registration immediately upon receipt of this solicitation.

(c) The Contractor is responsible for the accuracy and completeness of the data within the CCR, and for any liability resulting from the Government's reliance on inaccurate or incomplete data. To remain registered in the CCR database after the initial registration, the Contractor is required to confirm on an annual basis that its information in the CCR database is accurate and complete.

(d) Offerors and contractors may obtain information on registration and annual confirmation requirements via the Internet at http://www.ccr.gov or by calling 888-CCR–2423 (888–227–2423).

(End of clause)

[65 FR 50153, Aug. 17, 2000, as amended at 66 FR 53548, Oct. 23, 2001; 67 FR 30604, May 7, 2002]

1852.204–75 Security classification requirements.

As prescribed in 1804.404–70, insert the following clause:

SECURITY CLASSIFICATION REQUIREMENTS (SEP 1989)

Performance under this contract will involve access to and/or generation of classified information, work in a security area, or both, up to the level of _____ [insert the applicable security clearance level]. See Federal Acquisition Regulation clause 52.204–2 in this contract and DD Form 254, Contract Security Classification Specification, Attachment _____ [Insert the attachment number of the DD Form 254].

(End of clause)

[61 FR 40548, Aug. 5, 1996]

1852.204–76 Security Requirements for Unclassified Information Technology Resources.

As prescribed in 1804.470–4, insert a clause substantially as follows:

SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES, (JUL 2002)

(a) The Contractor shall be responsible for Information Technology security for all systems connected to a NASA network or operated by the Contractor for NASA, regardless of location. This clause is applicable to all or any part of the contract that includes information technology resources or services in which the Contractor must have physical or electronic access to NASA's sensitive information contained in unclassified systems that directly support the mission of the Agency. This includes information technology, hardware, software, and the management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems. Examples of tasks that require security provisions include:

(1) Computer control of spacecraft, satellites, or aircraft or their payloads;

(2) Acquisition, transmission or analysis of data owned by NASA with significant replacement cost should the contractor's copy be corrupted; and

(3) Access to NASA networks or computers at a level beyond that granted the general public, *e.g.* bypassing a firewall.

(b) The Contractor shall provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract. The plan shall describe those parts of the contract to which this clause applies. The Contractor's IT Security Plan shall be compliant with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 *et seq.*) and the Government Information Security Reform Act of 2000. The plan shall meet IT security requirements in accordance with Federal and NASA policies and procedures that include, but are not limited to:

(1) OMB Circular A–130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources;

(2) NASA Procedures and Guidelines (NPG) 2810.1, Security of Information Technology; and

(3) Chapter 3 of NPG 1620.1, NASA Security Procedures and Guidelines.

(c) Within ____days after contract award, the contractor shall submit for NASA approval an IT Security Plan. This plan must be consistent with and further detail the approach contained in the offeror's proposal or sealed bid that resulted in the award of this contract and in compliance with the requirements stated in this clause. The plan, as approved by the Contracting Officer, shall be incorporated into the contract as a compliance document.

(d)(1) Contractor personnel requiring privileged access or limited privileged access to systems operated by the Contractor for NASA or interconnected to a NASA network shall be screened at an appropriate level in accordance with NPG 2810.1, Section 4.5; NPG 1620.1, Chapter 3; and paragraph (d)(2) of this clause. Those Contractor personnel with non-privileged access do not require personnel screening. NASA shall provide screening using standard personnel screening National Agency Check (NAC) forms listed in paragraph (d)(3) of this clause, unless contractor screening in accordance with paragraph (d)(4) is approved. The Contractor shall submit the required forms to the NASA Center Chief of Security (CCS) within fourteen (14) days after contract award or assignment of an individual to a position requiring screening. The forms may be obtained from the CCS. At the option of the government, interim access may be granted pending completion of the NAC.

(2) Guidance for selecting the appropriate level of screening is based on the risk of adverse impact to NASA missions. NASA defines three levels of risk for which screening is required (IT–1 has the highest level of risk):

(i) IT–1—Individuals having privileged access or limited privileged access to systems whose misuse can cause very serious adverse impact to NASA missions. These systems include, for example, those that can transmit commands directly modifying the behavior of spacecraft, satellites or aircraft.

(ii) IT–2—Individuals having privileged access or limited privileged access to systems whose misuse can cause serious adverse impact to NASA missions. These systems include, for example, those that can transmit commands directly modifying the behavior of payloads on spacecraft, satellites or aircraft; and those that contain the primary copy of ''level 1'' data whose cost to replace exceeds one million dollars.

(iii) IT–3—Individuals having privileged access or limited privileged access to systems whose misuse can cause significant adverse impact to NASA missions. These systems include, for example, those that interconnect with a NASA network in a way that exceeds access by the general public, such as bypassing firewalls; and systems operated by the contractor for NASA whose function or data has substantial cost to replace, even if these